Advisory 2019-09

Security update for CODESYS V2.3 ENI server

Published: 23 October 2019

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2019-09_LCDS-319.docx

CONTENT

1 Affected Products

All CODESYS V2.3 ENI servers prior version V3.2.2.25 are affected. As the CODESYS ENI server is part of the CODESYS V2.3 setup, all CODESYS V2.3 setups prior V2.3.9.61 contain an affected version of the CODESYS ENI server.

2 Vulnerability overview

2.1 Type

Stack-based buffer overflow

2.2 Management Summary

A specific crafted request may cause a stack-based buffer overflow and could therefore execute arbitrary code on the CODESYS ENI server or lead to a denial-of-service condition due to a crash in the CODESYS ENI server.

2.3 References

CVE: CVE-2019-16265 [6]

CODESYS JIRA: LCDS-319

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as Critical.

The CVSS v3.0 base score of 10 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS ENI (CODESYS Standard Engineering Interface) server manages the objects of a CODESYS project in a central independent database system. A specific crafted ENI server request may cause a stack-based buffer overflow and could therefore execute arbitrary code on the CODESYS ENI server or lead to a denial-of-service condition due to a crash in the CODESYS ENI server.

3.2 Exploitability

This vulnerability could be exploited remotely, if the ENI server is licensed for remote access, in all other cases locally.

3.3 Difficulty

An attacker with low skills would be able to exploit this vulnerability.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability.

4 Available software updates

3S-Smart Software Solutions GmbH has released the CODESYS ENI server V3.2.2.25 to solve this vulnerability issue. This is part of the CODESYS setup V2.3.9.61.

Please visit the CODESYS update area for more information on how to obtain the software update [3].

Note: The previously released CODESYS ENI server V3.2.2.24 should already close the vulnerability. However, further tests by the researcher showed that the fix was incomplete. Therefore, we recommend to update the CODESYS ENI server again to version V3.2.2.25.

5 Mitigation

3S-Smart Software Solutions GmbH recommends using the available software update to fix the vulnerability.

Currently, 3S-Smart Software Solutions GmbH has not identified any specific workarounds for this vulnerability, in case the software update is not applied.

As part of a security strategy, 3S-Smart Software Solutions GmbH recommends the following general defense measures to reduce the risk of exploits:

- Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank Chen Jie from NSFOCUS for reporting this vulnerability following coordinated disclosure.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH CODESYS update area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-09_LCDS-319.pdf

Change History

Version	Description	Date
1.0	First version	12.09.2019
2.0	Additional fix necessary, fix version updated, CVE added	23.10.2019